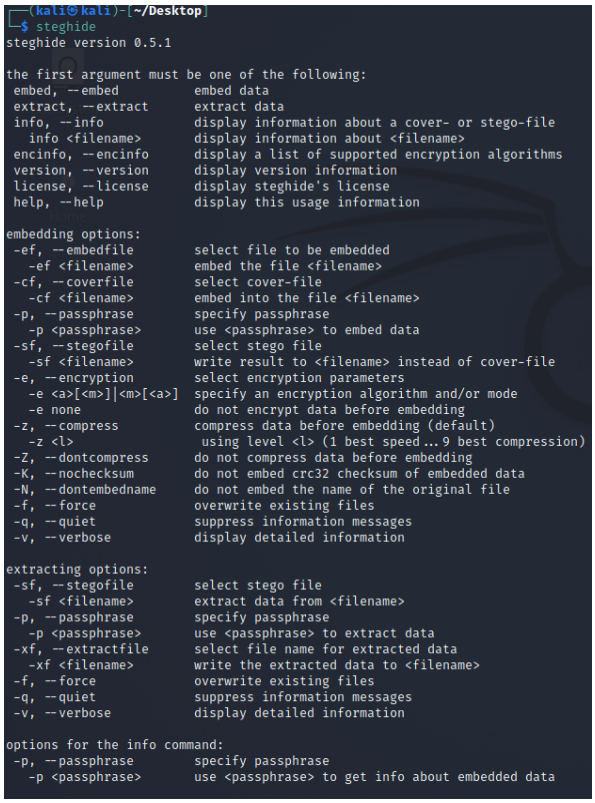
Lab 7

Steganography



Estimated time to complete: 40 Min

WHAT YOU WILL LEARN

Learn about what steganography is and how to find hidden messages hiding in plain sight. Use Steghide to create a hidden message and view a message hidden within an image.

WHY IT'S IMPORTANT

Understand how to be able to digitally hide a message within a message, and be able to extract hidden messages from a seemingly normal looking image.

SKILLS GAINED

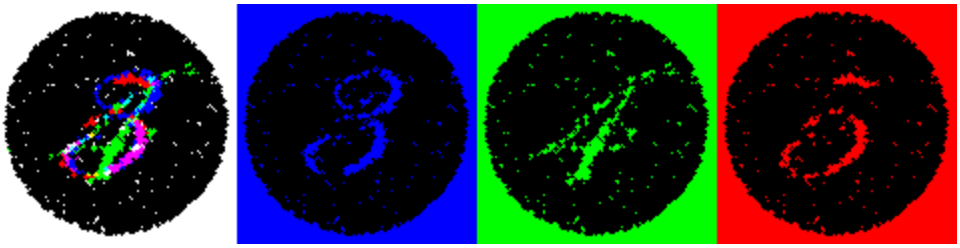
- Embedding hidden messages
- Viewing hidden messages
- How to use Steghide
- Identify images that may contain a hidden message

REQUIRED HARDWARE

- Raspberry Pi
- Internet Connection

WHAT IS STEGANOGRAPHY

Steganography is known as the practice of concealing a message within another message. An example of this that you've likely heard of before is using invisible ink to write a hidden message on a piece of paper. In the digital world, you can use steganography to conceal data within an ordinary looking file, such as an image or video. Steganography is different from cryptography as steganography hides data in plain sight. This makes it hard to detect that there is any hidden data at all whereas encrypted files, despite being harder to decrypt, are easily identifiable. One of the most common digital steganography techniques is to embed a text file within an image file.



HOW TO DETECT STEGANOGRAPHY

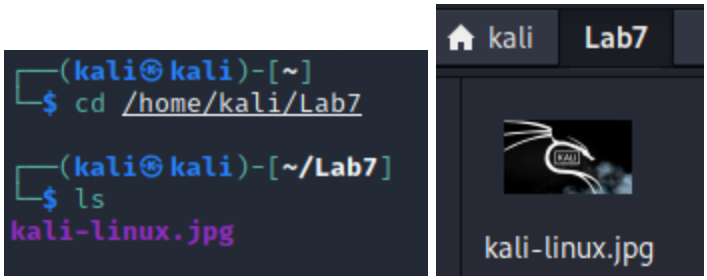
Searching for steganography is called steganalysis and is notoriously hard to do, even for digital forensics experts but we can look for some clues that would tip us off to steganography being used. Searching for steganography tools on the machine is probably the best way to tip us off that something is being hidden in images. Other things such as large file sizes (due to extra data being stored within them), weird files, and duplicate images can be clues as well. Duplicate files are very important to look for as we can compare between them to tell if something has changed, indicating a message might be hidden within.

CREATING STEGANOGRAPHY WITH STEGHIDE

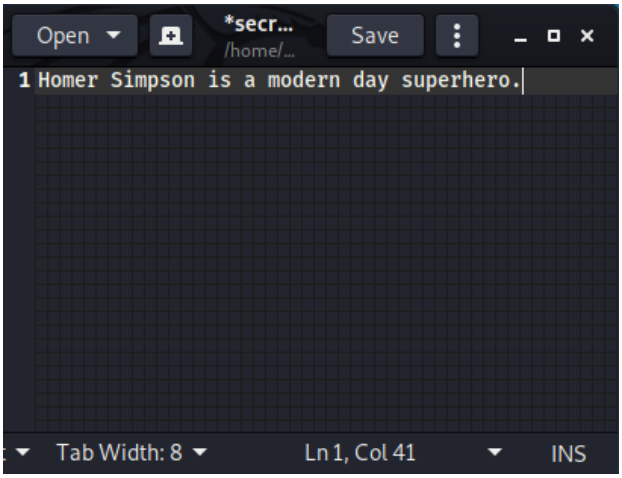
Steghide is a steganography tool available for linux. It allows users to both encrypt and decrypt data in images or audio with support for JPEG, BMP, WAV and AU files. It can also be used to detect images using steganography and give more information about a file. It uses passwords to protect the encrypted information and allow its users to store their information in plain sight.

STEP 1: HIDING TEXT

Now we are going to learn how to hide a secret text file inside of an image. Let's move over to the Lab7 folder to do this, open the terminal and use the command ***cd ~/Lab7*** to do this. Inside, you will find Kali-linux.jpg, this is the image we will be using to hide our secret.



Create a text file to hide in our image, to create and edit it, do ***gedit secret.txt*** and type in your secret message, you can then click save and exit the gedit window. Make sure this message isn't too long as if your data needs to be smaller than the file you are putting it in.



Now we should have kali-linux.jpg and secret.txt in our Lab7 folder (check with ***ls***). To hide our text in our image, run the following command (pick a pass of your choosing):

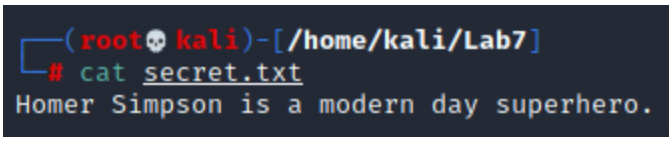
steghide embed -ef secret.txt -ef kali-linux.jpg -p <password>

Our secret text file is now embedded and hidden inside of our image, we can now delete the secret text file by doing ***rm secret.txt***. To get info about the hidden message, you can do ***steghide info kali-linux.jpg***.

```
┌──(root💀kali)-[/home/kali/Lab7]
└─# steghide info kali-linux.jpg
"kali-linux.jpg":
  format: jpeg
  capacity: 3.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "secret.txt":
    size: 41.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

STEP 2: VIEWING HIDDEN TEXT

To decrypt our text file from our image we can do the command ***steghide extract -sf kali-linux.jpg,*** this will actually remake our secret.txt file in the same directory, you can open it with ***cat secret.txt*** to verify it is the same message.



EXERCISE:

1: Find the hidden text

Put your shoes in the place of a digital forensics investigator, you are investigating a mysterious hacking group called Cicada 3301, known for their steganography internet recruiting challenges. Your team followed one of the members to DefCon, an annual hacker conference held in Las Vegas, Nevada, and managed to capture the suspects password using a Wifi Pineapple. The password recovered was ***DontLetTheFlameDieOut!*** . We know the suspect was communicating with other members of Cicada during the conference, do some research on DefCon and see if you can find some clues to tell you where to find the secret message hidden somewhere inside the **~/Lab7/Exercise** directory.

TIP: Make sure your gedit window is fullscreen! You might not see the full message otherwise.

REVIEW

1: How could you suspect that steganography is used?

A) Using a steghide info command

B) Noticing duplicate files of different sizes

C) Seeing Steganography tools installed on a device

D) All of the above

2: Steganography is different from Cryptography because

A) It makes text hard to find

B) Often requires a key or password to find the original text

C) Steganography hides data in images or audio

D) It tries to hide information

3: Detecting steganography is easy (True/False)

4: Steghide doesn't support what type of file?

A) GIF

B) BMP

C) AU

D) JPEG

5: You can only encrypt data in a file if the data is smaller than the file you are putting it in (True/False)

6: You can view the content of a steganography file without a password (True/False)

Answers: 1:D 2:C 3:F 4:A 5:T 6:F